Assistant Secretary of Defense John Plumb and Army General Paul Nakasone, commander of U.S. Cyber Command, prepare their testimony for House Armed Services Committee, in Washington, DC, March 30, 2023 (DOD/E.J. Hersom)

Letter to the Editor

The April 2023 issue of *Joint Force Quarterly* includes a positive review of our recent book, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, by Stafford Ward, as well as an article on cyber and deterrence by James Van de Velde. Readers, both those who follow the cyber and deterrence discussion closely and those new to the topic, might be confused by the two pieces and their disparate representation of U.S. Cyber Command's operational approach of persistent engagement and how it fits with a strategy of deterrence and with the more recent concept of integrated deterrence. As theorists writing on cyber persistence and a practitioner implementing persistent engagement, we offer some clarification.

Stafford Ward's review accurately describes our thesis, derived from historical experience, that states misunderstanding the technical, tactical, and operational features of the strategic environment in which they seek security may suffer strategic losses in competition, crisis, and armed conflict. We introduced the analytical construct of three strategic environments—conventional, nuclear, and cyber—in which each relies on a distinct logic for producing security. In cyberspace, security rests primarily on the strategic principle of initiative persistence in exploitation—anticipating the exploitation of one's own vulnerabilities, leveraging the capacity to exploit others' vulnerabilities, and seizing and sustaining the initiative in this exploitation dynamic. Security in this interconnected space of constant contact and fluid technological terrain requires continuous maneuvering against adversaries to gain insights about adversary tactics, techniques, and procedures. These insights can be shared with government and industry partners at home and abroad to enable them to proactively inoculate vulnerable assets from cyber exploitation, disruption, and destruction, leading to increased and improved resiliency and defense. These insights can also be used to preclude, inhibit, and otherwise constrain adversaries from cumulating strategic gains.

Deterrence, which rests on prospective threat to react (through threat of either punishment or attritional denial), has failed as a strategy in cyberspace both to support resiliency and defense and to dissuade states from pursuing strategic gains cumulatively in and through cyberspace below the level of armed conflict. Cyber operations and campaigns conducted in competition are more than a nuisance or mere espionage—they can be strategically consequential. As an example, the North Koreans are undermining the effectiveness of the U.S.'s Ground-based Midcourse Defense System by funding North Korea's missile and nuclear programs via strategic cyber campaigns that manipulated digital financial transactions. This is why the Department of Defense and U.S. Cyber Command adopted the Defend Forward strategy and the operational approach of persistent engagement in 2018. The 2022 U.S. National Defense Strategy reinforces this paradigm shift in its call for campaigning below armed conflict to limit, frustrate, and disrupt competitor activities that seriously affect U.S. interests. In other words, persistent engagement is *not* the "operational implementation of cyber deterrence" as Van de Velde concludes. Persistent engagement is an alternative to a deterrence strategy. Although we argue in *Cyber Persistence Theory* that deterrence as a strategic approach may succeed against armed attack equivalent effects delivered in and through cyberspace, it patently does not provide security below that threshold, and an alternative approach based on a distinct strategic logic must guide the pursuit of security in that strategic space. When employed persistently over time, a "deterrent effect" might result from cyber campaigns, but this is not because one has applied a deterrence strategy.

These nuances are critically important for civilian and military scholars, policymakers, and students to grasp. Calling cyberspace operations "the operational implementation of cyber deterrence" is not only incorrect but also potentially distracting at a time when strategic clarity is required.

Cyber capabilities and operations must be leveraged to support integrated deterrence in a way that aligns with the reality of the cyberspace strategic environment. Unlike conventional and nuclear capabilities, cyber activities alone do not deter because they are not useful as a coercive

mechanism. This conclusion follows from empirical evidence and scholarly consensus. Accordingly, the best use of cyberspace capabilities and operations for integrated deterrence comes from their persistent use in "campaigning" against continuously active adversaries, working across boundaries (interagency, private sector, and allies) with all instruments of national power to set conditions to deter and prevail in crisis and conflict. Strategic value comes not from signaling intent and shaping decisionmaking in those moments but from advancing security through cyber means applied in competition to structure the crisis or fight.

There are several threads to setting conditions for crisis or conflict through campaigning. The first involves defensive activities to set the theater and globe for joint force operations. This includes mission assurance of one's own networks, weapons, and systems, as well as coalition warfighting networks. The second thread is setting partnerships. As General Paul Nakasone articulated in his recent Vanderbilt University keynote address, "The winners of future competitions and conflicts will be those coalitions that can set conditions for dynamic collaboration with speed across a broader section of societies, regions, and sectors, fostering mutual understanding and congruent action." The third thread is the effort to undermine the adversary's desired crisis and warfighting conditions and constrain its freedom of maneuver. Campaigning in and through cyberspace can undermine an adversary's confidence in its capabilities, complicate military preparations, counter information campaigns that aim to undermine U.S. public support and alliance cohesion, expose information and intelligence to deny the adversary control of the global narrative, and preclude or constrain opportunities through hunt-forward operations.

Examples of these threads include the hunt-forward operations in Montenegro to improve American cyber defenses ahead of the 2020 election and those in Ukraine to provide and receive insights to/from Ukrainian operators while also inoculating U.S. systems from Russian cyber actors and any proxies supporting its war against Ukraine. Additionally, after discovering a massive Russian botnet (CyclopsBlink) that had not yet been activated against U.S. national interests, the Federal Bureau of Investigation effectively dismantled the botnet in March 2022. Finally, U.S. cyber-enabled campaigns through public release of intelligence have been credited with ensuring alliance stability for a coordinated effort to compel Russia to cease its aggression.

In our book, as Ward notes, we are cautious in making claims that cannot be supported by evidence or compelling logic. Cyber is a novel capability that has never been used in a militarized crisis between nuclear-armed peers. In a crisis, uncertainty invites miscalculation and inadvertent escalation, and novel cyber actions could introduce a bevy of uncertainties in signaling, effects, shared understandings of the severity of effects, and commitment. The assertion that cyber provides "off-ramps" to deescalate crisis is untested, unproved, not empirically supported, and counter to theories of crisis bargaining. We do not know whether cyber options in a crisis would signal lack of resolve or if they would deescalate or escalate the situation. While cyber has proved to be nonescalatory in day-to-day competition between nuclear-armed peers, this does not ipso facto mean cyber is nonescalatory or deescalatory in a crisis.

Finally, we urge readers to recognize that these arguments are more than purely academic—they inform decisions about resourcing, force structure, and mission. To that end, we disagree with Van de Velde's claim that persistence in competition vies with posturing for contingency. The reality is far more nuanced. First, as we describe earlier, campaigning in competition enables warfighting. Second, there is a great deal of overlap and synergy between the requirements for day-to-day competition and posturing for contingency. For example, campaigning helps secure the Department of Defense information networks, readies the force, increases whole-of-nation resilience, uncovers targets of opportunity, and generates response options for use in crisis or conflict. There are indeed priorities specific to managing crisis and prevailing in conflict, such as access to specialized hard targets and the bespoke tools to exploit those targets. Although effort must surely be expended on tailored accesses and capabilities, campaigning helps ensure they can be brought to bear in the event of crisis and armed conflict. Campaigns in competition are not less consequential than actions in crisis and armed conflict, as implied by the figures in Van de Velde's article.

Cyberspace requires us to rethink the competition-conflict continuum, which is often depicted linearly from competition to crisis to conflict, with risk increasing as one moves along the continuum. The implication is that war presents the greatest risk of strategic loss, and therefore everything we resource and execute in competition is weighed against the likelihood of escalation to war, as well as how it postures and prepares us for war. As argued in *Cyber Persistence Theory*, competition in and through cyberspace can hold the same strategic import as armed conflict. Thinking about competition principally as a step toward armed conflict neglects the ways in which actions in competition can secure strategic victory without ever having to engage in armed conflict.

We appreciate Stafford Ward's encouraging *JFQ* readers to examine our book for a fuller discussion of cyber competition, deterrence, initiative persistence, and persistent engagement. We agree with the National Defense Strategy and James Van de Velde that ensuring adversaries cannot use conventional force, nuclear threats, and exploitative cyber campaigns to undermine U.S. power certainly requires an integrated approach. But contrary to Van de Velde's suggestion, one must also acknowledge that different approaches are needed for different threats. Initiative persistence is not deterrence—it is distinct and, if pursued well, complementary and supportive. **JFQ**

Michael P. Fischerkeller, Researcher, Institute for Defense Analyses; Emily O. Goldman, Cyber Strategist at U.S. Cyber Command; Richard J. Harknett, Chair, Center for Cyber Strategy and Policy at the University of Cincinnati